PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) **Internationale Patentklassifikation** 7 :
H04L 9/08

A1

(11) **Internationale Veröffentlichungsnummer:** **WO 00/22776**

(43) **Internationales Veröffentlichungsdatum:** 20. April 2000 (20.04.00)

(21) **Internationales Aktenzeichen:** PCT/EP99/07052

(22) **Internationales Anmeldedatum:** 22. September 1999 (22.09.99)

(30) **Prioritätsdaten:**
198 47 944.1 9. Oktober 1998 (09.10.98) DE

(71) **Anmelder** *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) **Erfinder; und**
(75) **Erfinder/Anmelder** *(nur für US)*: SCHWENK, Jörg [DE/DE]; Südwestring 27, D–64807 Dieburg (DE).

(74) **Gemeinsamer Vertreter:** DEUTSCHE TELEKOM AG; Patentabteilung R151, D–64307 Darmstadt (DE).

(81) **Bestimmungsstaaten:** HU, IL, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) **Title:** METHOD FOR ESTABLISHING A COMMON KEY BETWEEN AN EXCHANGE AND A GROUP OF SUBSCRIBERS

(54) **Bezeichnung:** VERFAHREN ZUM ETABLIEREN EINES GEMEINSAMEN SCHLÜSSELS ZWISCHEN EINER ZENTRALE UND EINER GRUPPE VON TEILNEHMERN

(57) **Abstract**

The aim of the invention is to provide a method for establishing a common key between an exchange and a group of at least three subscribers, which has the same security standards as the DH method. The inventive method is based on a publicly known mathematical number group (G) and an element of the group $g \in G$ of a large order. Each of the n subscribers produces a random number (i), calculates the value of g^i in G and transmits this value to the exchange (Z). Another random number (z) is generated in the exchange (Z) and the values $(g^i)^z$ in G are calculated. The shares are derived from these values using a threshold method and an (n,2n–1)–threshold method is constructed from these. The exchange (Z) transfers the shares produced to the n subscribers, together with the values $(g^i)^z$ and the subscribers can then reconstruct the key (k) using the (n,2n–1)–threshold method. The inventive method is particularly advantageous for producing a cryptographic key for a group of several, but at least 3, subscribers.

(57) **Zusammenfassung**

Das vorliegende Verfahren zur Erfindung eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von mindestens drei Teilnehmern soll den gleichen Sicherheitsstandard wie das DH–Verfahren aufweisen. Das Verfahren basiert auf einer öffentlich bekannten mathematischen Zahlengruppe (G) und einem Element des Gruppe $g \in G$ großer Ordnung. Jeder der n Teilnehmer erzeugt eine Zufallszahl (i), berechnet den Wert von g^i in G und sendet diesen Wert an die Zentrale (Z). In der Zentrale (Z) wird ebenfalls eine Zufallszahl (z) generiert und die Werte $(g^i)^z$ in G berechnet. Aus diesen Werten werden die shares anhand eines Threshold–Verfahrens abgeleitet und aus ihnen ein (n,2n–1)–Threshold–Verfahren konstruiert. Durch die Zentrale (Z) werden die erzeugten shares zusammen mit den Werten $(g^i)^z$ an die n Teilnehmer übertragen, die über das (n,2n–1)–Threshold–Verfahren den Schlüssel (k) rekonstruieren können. Das erfindungsgemäße Verfahren läßt sich vorteilhaft zur Erzeugung eines kryptografischen Schlüssels für eine Gruppe von mehreren, mindestens jedoch drei Teilnehmern einsetzen.